AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT

1. CONTRACT ID CODE	PAGE OF PAGES
	1 7

2. AMENDMENT/MODIFICATION NO.	3. EFFECTIVE DATE	4. REQUISITION/PURCHASE REQ. NO.	5. PROJECT NO. (If applicable)
014	05/08/2013	PR-OEI-13-00447	

6. ISSUED BY CODE RTPPOD

RTPPOD
US Environmental Protection Agency
109 T.W. Alexander Drive
Mail Code: E105-02
Research Triangle Park NC 27709

7. ADMINISTERED BY (If other than Item 6) CODE

8. NAME AND ADDRESS OF CONTRACTOR (No., street, county, State and ZIP Code)

CGI FEDERAL INC.
12601 FAIR LAKES CIRCLE
GWAC SOLUTIONS CENTER
FAIRFAX VA 220334902

CODE 145969783 FACILITY CODE

(x) 9A. AMENDMENT OF SOLICITATION NO.

9B. DATED (SEE ITEM 11)

X 10A. MODIFICATION OF CONTRACT/ORDER NO.
GS35F4797H
EP-G11D-00056

10B. DATED (SEE ITEM 13)
03/24/2011

11. THIS ITEM ONLY APPLIES TO AMENDMENTS OF SOLICITATIONS

The above numbered solicitation is amended as set forth in Item 14. The hour and date specified for receipt of Offers is extended, is not extended.
Offers must acknowledge receipt of this amendment prior to the hour and date specified in the solicitation or as amended, by one of the following methods: (a) By completing Items 8 and 15, and returning _____ copies of the amendment; (b) By acknowledging receipt of this amendment on each copy of the offer submitted; or (c) By separate letter or telegram which includes a reference to the solicitation and amendment numbers. FAILURE OF YOUR ACKNOWLEDGEMENT TO BE RECEIVED AT THE PLACE DESIGNATED FOR THE RECEIPT OF OFFERS PRIOR TO THE HOUR AND DATE SPECIFIED MAY RESULT IN REJECTION OF YOUR OFFER. If by virtue of this amendment you desire to change an offer already submitted, such change may be made by telegram or letter, provided each telegram or letter makes reference to the solicitation and this amendment, and is received prior to the opening hour and date specified.

12. ACCOUNTING AND APPROPRIATION DATA (If required)
See Schedule Net Increase: $250,263.44

13. THIS ITEM ONLY APPLIES TO MODIFICATION OF CONTRACTS/ORDERS. IT MODIFIES THE CONTRACT/ORDER NO. AS DESCRIBED IN ITEM 14.

CHECK ONE	
	A. THIS CHANGE ORDER IS ISSUED PURSUANT TO: (Specify authority) THE CHANGES SET FORTH IN ITEM 14 ARE MADE IN THE CONTRACT ORDER NO. IN ITEM 10A.
	B. THE ABOVE NUMBERED CONTRACT/ORDER IS MODIFIED TO REFLECT THE ADMINISTRATIVE CHANGES (such as changes in paying office, appropriation date, etc.) SET FORTH IN ITEM 14, PURSUANT TO THE AUTHORITY OF FAR 43.103(b).
	C. THIS SUPPLEMENTAL AGREEMENT IS ENTERED INTO PURSUANT TO AUTHORITY OF:
X	D. OTHER (Specify type of modification and authority) Mututal Agreement of the Parties

E. IMPORTANT: Contractor X is not, is required to sign this document and return _____ copies to the issuing office.

14. DESCRIPTION OF AMENDMENT/MODIFICATION (Organized by UCF section headings, including solicitation/contract subject matter where feasible.)

DUNS Number: 145969783+4797
TOPO: David Sczepanski Max Expire Date: 09/30/2016
The purpose of this modification is to:
1) Revise the Performance Work Statement to add Access Control tasks
2) Add labor in accordance with the revised Performance Work Statement
3) Incrementally Fund Option Period II

See attached revised Performance Work Statement and revised CLINs. All other terms and conditions remain unchanged.

Total Amount for this Modification: $1,136,461.34
Continued ...

Except as provided herein, all terms and conditions of the document referenced in Item 9A or 10A, as heretofore changed, remains unchanged and in full force and effect.

15A. NAME AND TITLE OF SIGNER (Type or print)		16A. NAME AND TITLE OF CONTRACTING OFFICER (Type or print)	
		Laconda S. Cannady	
15B. CONTRACTOR/OFFEROR (Signature of person authorized to sign)	15C. DATE SIGNED	16B. UNITED STATES OF AMERICA Laconda S Cannady (Signature of Contracting Officer)	16C. DATE SIGNED 05/08/2013

NSN 7540-01-152-8070
Previous edition unusable

STANDARD FORM 30 (REV. 10-83)
Prescribed by GSA
FAR (48 CFR) 53.243

NAME OF OFFEROR OR CONTRACTOR
CGI FEDERAL INC.

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	New Total Amount for this Version: $26,299,699.22 New Total Amount for this Award: $36,245,591.16 Obligated Amount for this Modification: $250,263.44 New Total Obligated Amount for this Award: $12,241,533.59 Incremental Funded Amount changed: from $11,991,270.15 to $12,241,533.59 CHANGES FOR LINE ITEM NUMBER: 3-Option Period II Total Amount changed from $6,084,613.35 to $6,334,876.79 Obligated Amount for this modification: $250,263.44 Incremental Funded Amount changed from $4,535,000.00 to $4,785,263.44 CHANGES FOR DELIVERY LOCATION: OEI/RTP/NCC Amount changed from $6,084,613.35 to $6,334,876.79 NEW ACCOUNTING CODE ADDED: Account code: 13--WR-H1NNIT3-ZZZHF8-2504-CAS00011--13H1KER003-001 Beginning FiscalYear 13 Ending Fiscal Year Fund (Appropriation) WR Budget Organization H1NNIT3 Program (PRC) ZZZHF8 Budget (BOC) 2504 Job # (Site/Project) CAS00011 Cost Organization DCN-LineID 13H1KER003-001 Quantity: 0 Amount: $150,000.00 Percent: 2.36784 Subject To Funding: N Payment Address: RTP Finance Center US Environmental Protection Agency RTP-Finance Center (D143-02) 109 TW Alexander Drive Durham NC 27711 NEW ACCOUNTING CODE ADDED: Account code: 13--WR-H1NNIT3-ZZZHF8-2512-CKE00009--13H1KER003-002 Continued ...				

ITEM NO (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	Beginning FiscalYear 13 Ending Fiscal Year Fund (Appropriation) WR Budget Organization H1NNIT3 Program (PRC) ZZZHF8 Budget (BOC) 2512 Job # (Site/Project) CKE00009 Cost Organization DCN-LineID 13H1KER003-002 Quantity: 0 Amount: $100,263.44 Percent: 1.58272 Subject To Funding: N Payment Address: RTP Finance Center US Environmental Protection Agency RTP-Finance Center (D143-02) 109 TW Alexander Drive Durham NC 27711 CHANGES FOR LINE ITEM NUMBER: 4-Option Period III Total Amount changed from $6,219,865.35 to $6,684,809.65 CHANGES FOR DELIVERY LOCATION: OEI/RTP/NCC Amount changed from $6,219,865.35 to $6,684,809.65 CHANGES FOR LINE ITEM NUMBER: 5-Option Period IV Total Amount changed from $6,358,374.63 to $6,566,400.98 CHANGES FOR DELIVERY LOCATION: OEI/RTP/NCC Amount changed from $6,358,374.63 to $6,566,400.98 CHANGES FOR LINE ITEM NUMBER: 6-Option Period V Total Amount changed from $6,500,384.55 to $6,713,611.80 CHANGES FOR DELIVERY LOCATION: OEI/RTP/NCC Amount changed from $6,500,384.55 to $6,713,611.80 Delivery Location Code: OEI/RTP/NCC OEI/RTP/NCC US Environmental Protection Agency 109 TW Alexander Dr. Research Triangle Park NC 27709 USA Continued ...				

NAME OF OFFEROR OR CONTRACTOR
CGI FEDERAL INC.

ITEM NO (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	Payment: RTP Finance Center US Environmental Protection Agency RTP-Finance Center (D143-02) 109 TW Alexander Drive Durham NC 27711 FOB: Destination Period of Performance: 04/01/2011 to 09/30/2016				

GS-35F-4797H, TASK ORDER
EPG11D00056
Modification # 14

MODIFICATION TO THE CONTRACT

1. The clause entitled "INCREMENTAL FUNDING" has been modified. The text is as follows:

This contract is incrementally funded. Modification #14 to this order is adding $250,263.44 increasing the amount for Option Period II from $4,535,000.00to $4,785,263.44. The amount presently available for payment and allotted to the contract is $4,785,263.44for Option Period II and will cover performance through July 30, 2013.

2. The clause entitled "Limitation of Government's Obligation" has been modified. The text is as follows:

(a)This task order is incrementally funded. For this item, the sum of $4,785,263.44 of the total price is presently available for payment and allotted to this contract for Option Period II.

(b) For items identified in paragraph (a) of this clause, the Contractor agrees to perform up to the point at which the total amount payable by the Government, including reimbursement in the event of termination of those items for the Government's convenience, approximates the total amount currently allotted to the contract. The Contractor will not be obligated to continue work on those items beyond that point. Subject to the clause entitled, "Termination for Convenience of the Government", the Government will not be obligated in any event to reimburse the Contractor in excess of the amount payable by the Government in the event of termination of applicable contract line items for convenience includes costs, profit, and estimated termination costs for those line items.

(c) Notwithstanding the dates specified in the allotment schedule in paragraph (i) of this clause, the Contractor will notify the Contracting Officer, in writing, at least 5 days prior to the date when, in the Contractor's best judgment, the work will reach the point at which the total amount payable by the Government, including any cost for termination for convenience, will approximate 85% of the total amount them allotted to the contract for performance of the applicable items. The notification will state (1) the estimated date when that point will be reached and (2) an estimate of additional funding, if any, needed to continue performance of applicable line items up to the next scheduled date for allotment of funds identified in paragraph (i) of this clause, or to a substitute date as determined by the Government pursuant to subparagraph (d) of this clause. If after such notification, additional funds are not allotted by the date identified in the Contractor's notification, or by an agreed substitute date, the Contracting Officer will terminate any item(s) for which additional funds have not been allotted, pursuant to the clause entitled "Termination for Convenience of the Government."

(d) The parties contemplate that the Government will allot additional funds for continued performance of the contract line items identified in paragraph (a) for this clause and will determine the estimated period of contract performance which will be covered by the funds. The provisions of paragraphs (b) through (d) of this clause will apply in like manner to the additional allotted funds and to the new estimated period of contract performance. The contract will be modified accordingly.

(e) If, solely by reason of failure of the Government to allot additional funds, by the dates indicated below, in amounts sufficient for timely performance of the contract line items identified in paragraph (a) of this clause, the Contractor incurs additional costs or is delayed in the performance of the work under this contract and if additional funds are allotted, an equitable adjustment will be made in the price of the items, or in the time of delivery, or both. Failure to agree to any such equitable adjustment hereunder will be a dispute concerning a question of fact within the meaning of the clause entitled "Disputes."

(f) The Government may at any time prior to termination allot additional funds for the performance of the contract line items identified in paragraph (a) of this clause.

(g) The termination provisions of this clause do not limit the rights of the Government under the clause entitled "Default". The provisions of this clause are limited to the work and allotment of funds for the contract line items set forth in paragraph (a) of this clause. This clause no longer applies once the contract is fully funded except with the regard to the rights or obligations of the parties concerning equitable adjustments negotiated under paragraph (d) or (e) of this clause.

(h) Nothing in this clause affects the right of the Government to terminate this contract pursuant to the contract clause entitled "Termination for Convenience of the Government".

(i) The parties contemplate that the Government will allot funds to this contract incrementally as follows:

Performance Period	Modification	Cost Ceilings NTE
Base Period	0	$3,315,270.15
Base Period	11	($166,000.00)
Base Period	12	($1,000,000.00)

Base Period Total: $2,149,270.15

Remaining Balance for Base Period: $1,184,535.00

Option Period I	2	$1,200,000.00
Option Period I	3	$3,500,000.00
Option Period I	9	$275,000.00
Option Period I	11	$166,000.00
Option Period I	12	$166,000.00

Option Period I Total: $5,307,000.00

Remaining Balance for Option Period I is $1,305,086.79

Option Period II	10	$1,290,000.00
Option Period II	13	$3,245,000.00
Option Period II	14	$ 250,263.44

Option Period II Total: $4,785,263.44

Remaining Balance for Option Period II is $1,299,349.91

The amount presently available for payment and allotted to the contract is $4,785,263.44for Option Period II and will cover performance through July 30, 2013.

Attachment #2

PERFORMANCE WORK STATEMENT (PWS) REVISED 04/2013 CONFORMED COPY

3.1 Background

The National Computer Center (NCC) provides computing, telecommunications services, and technology support for the Agency. This operations environment includes support for computing and associated services with other Federal agencies, state and local environmental offices, as well as EPA contractors and grantees. Additionally, EPA has a Federal mandate to make certain data available and accessible to the public. The diversity of this mission and customer requirements creates unique challenges for networking and securing the Agency's IT resources and data.

EPA currently has multiple tasks performing disparate functions that will be combined under this TO. EPA intends to combine the technical operations and maintenance components of the **WAN Telecommunications Operations** and **NCC Security Management** under a **Network Operations Security Center (NOSC)**, with key personnel located within the NCC at Research Triangle Park (RTP), NC. The NOSC shall provide continuous monitoring and oversight of the EPA WAN, NCC operations, and security operations. All other requirements (i.e., other than operations) do not mandate physical location of personnel within the NCC. A key requirement for contractor proposals is a design and implementation strategy for a combined NOSC, including discussions on management and organizational structure, tactical operations plan, functional separation of duties, required tools and technologies, and anticipated staffing. Additionally, each contractor proposal shall describe how the on-going operational support requirements for WAN telecommunications and security will be accomplished.

To summarize, contractors shall provide an integrated and comprehensive project plan, including a critical path analysis and schedule, to address each of the four key areas below:

- Data Telecommunications Operational Support for the EPA WAN
- Security Operational Support for the EPA WAN and the NCC
- Detailed plan of execution for migrating existing network and security functions into a NOSC
- Proposed solution and methodology for operation and support of a NOSC

The paragraphs below summarize the current operational model and functional requirements of EPA's **WAN Telecommunications Operations** and **NCC Security Management**. These descriptions are intended to benchmark the current scope of requirements within these technical areas. Contractors are reminded that some re-distribution of functional requirements across different contracts is likely during the term of this TO. Innovative and recognized strategies for

improving the economies and efficiencies of telecommunications and security operations are to be included as well.

Current **WAN Telecommunication Operations** is responsible for providing day-to-day operations and maintenance for the EPA Wide Area Network (WAN) connecting the 10 U.S. Regions (including Alaska, Hawaii and Puerto Rico), research laboratories, Washington, D.C. Headquarters, and RTP sites. These responsibilities include managing implementation of new requirements via the present Telecommunication Service Request (TSR) process, operating the RTP-based Network Control Facility (NCF), and providing second level Network Technical Support (NTS). WAN first level support is provided by the NCF, where active monitoring of the network is done and initial network trouble calls are received. The NCF is currently located within the computer room of the NCC. If necessary, the NCF escalates troubleshooting to second level support in the Network Telecommunications Services (NTS) group. **WAN Telecommunications Operations** provides design, procurement, installation, upgrade/changes, documentation, reporting, and ongoing maintenance support. Further, it manages and coordinates with support contractors and telecommunications services contractors to provide circuits, services, hardware/software, maintenance, billing/dispute resolution, and problem resolution. Currently, circuit hardware, software, service orders, and billing/dispute resolution are provided jointly by EPA, the current ITS-EPA contractor, Computer Sciences Corporation, and a secondary support contractor, ECS under the ITS-ACT contract, GS-06F-0332Z, Delivery Order #15. The current support contractor manages the EPA-owned routers, central switches, telecom servers/appliances, and telecom diagnostic equipment. Primary contract support includes:

- Support for WAN operations including moves, additions, and other changes, and network service restoration.
- Support for a Request for Change/Telecommunications Service Request system to manage incoming WAN work requests.
- Procurement of hardware, software, supplies, maintenance, and other telecommunications services when advantageous for the government.
- Circuit provisioning and billing/dispute resolution, and tracking of service level agreement (SLA) failure credits for the bulk of the present network. Residual Federal Telecommunications Service (FTS) circuits and a small number of circuits, provisioned under the General Services Administration (GSA) NETWORX contract, are managed by ECS under contract GS00T07NSD0041. EPA expects these functions to be merged under EPA's WAN2010 NETWORX contract award, which is imminent. EPA expects the circuits remaining under FTS and the old NETWORX contract to be migrated to the WAN2010 NETWORX provider.
- Documentation including network diagrams, procedures, recommendations, problem root cause analysis, reports, inventories and support for response to audits.

- Design, installation, testing, configuration and operations/maintenance of the Cisco ISE, NCS and MSE into EPA's production network. Phase I support will focus on WLAN usage. Installation of the devices will be in RTP and DC.

- NSOC will produce documentation (SCD, Security Plan, SOP, etc…) for the NAC devices.
- NSOC will work with other groups and task orders for integration of directory authentication services into the NAC deployment.
- NSOC will assist identified task orders in verifying the WLAN Supplicant is FIPS compliant and all traffic from PC to back end WiSM2 device is encrypted with FIPS 140-2 level encryption. Use of NAC for end point control (desktop) will be considered a phase II (FY14) item.
- NSOC will assist identified task orders in creation and review of Windows Supplicant for WLAN Type 1(GFE), 2(EPA BYOD), 3(Guest) users.
- Provide and support NATing on RTP and DC firewall(s) to support type 1, 2 and 3 WLAN users Internet access. Port starvation should be considered with migration to Office365. No more than 2000 private IPs per public NATed IP.
- NATing firewall data should be sent to Arcsight.
- EDSD will work with TISS to address monitoring of NAT data within Arcsight.
- Test NAT fail over between RTP to DC and DC to RTP.
- Work with NCC, AT&T and EDSD on QOS options for type 2 and 3 WLAN users. This requirement will need to consider impact of Office365 traffic and IPv6 on QOS settings.

From time to time, the contractor must respond to certain incidents under this Task Order which would require the deployment of person(s) to physically work on network equipment in the NCC, within thirty minutes of the incident.

With the award of the WAN2010 solicitation, the provisioning, maintenance, and operation of all WAN routers will be transitioned to a managed service. EPA fully expects this managed service to significantly reduce the number of primary contractor support engineering labor hours necessary to support the WAN. However, some residual level of primary support engineering expertise will still be required for network troubleshooting, NCC and EPA Headquarters MAN support, and interfacing with the WAN2010 NETWORX provider. Occasionally, field travel is required to support EPA conference network set up and operation, EPA site surveys, engineering, implementation, or troubleshooting. Physical access and meetings will still be required, but a reduced local presence and increased remote access to the network is envisioned and the change in support structure is expected. Secure remote system administration is ongoing and expected by network support personnel and other support contractor staff.

NCC Security Management is responsible for ensuring adequate logical protection for systems, network-attached resources, and data assets of the Agency. Physical protection is the responsibility of facilities management organizations, with possible technical consulting from the NCC for specialized physical security requirements involving the centralized data center. Due to the Agency's highly distributed network topology, security management responsibilities must be decentralized to some degree. Local system administrators (SAs) and local area network (LAN) administrators throughout the Agency programs, Regional offices, and laboratories share the security management responsibilities for the logical protection of their locally managed resources. NCC's Security Management team defines its scope of

responsibility to cover the centralized assets within the NCC, the wide area network (WAN) providing connectivity among the distributed sites, and the distributed network routers that mark the connectivity transition between the WAN and the LAN environment at the distributed sites.

The objectives of **NCC Security Management** are to provide the technical operations and support the operations security management requirements for the centrally managed computing environment, the Agency WAN environment, and the technical assistance and support to the operations security requirements of the Agency distributed systems environment. Today, the scope of these requirements involves two operations security management areas: (1) **Security Technical Operations**, which covers the operations and maintenance of EPA's network security infrastructure devices (e.g., firewalls, intrusion detection system/intrusion prevention system (IDS/IPS) sensors, security appliances, security management and monitoring equipment) for the WAN and the NCC; and (2) **Operations Security Program Management**, which covers security operations oversight and monitoring, security management and reporting, security assessment and consulting, and security audits support for the WAN and the NCC.

Security Technical Operations provides security management using industry best practices and by applying risk management concepts and theories that effectively manage and monitor EPA's IT security infrastructure. Security functions also include providing engineering support in the configuration, management, audit and operation of security components including, but not limited to, firewalls, IDS/IPS, authentication servers, Virtual Private Networks (VPN), Network Access Control (NAC) and server/network vulnerability and assessment tools. **Security Technical Operations** is responsible for, and uses, the Firewall Rule Request (FRR) process to provide customer support in development and review of firewall rules. This process is used to ensure requests are technically correct, accurate, and any associated risks are quantified.

EPA has two active points of presence to the Internet. Each is protected by a formal firewall complex (load balanced with failover capability). A co-located Continuity of Operations site (COOP)/Disaster Recovery (DR) site (currently in Boulder, Colorado) is updated and tested as appropriate such that, if activated, the rule set and controls will allow safe operation of DR facilities. Specific functions related to firewall system management include:

- Perform administration, management, and support of production firewall clusters and test lab systems.
- Provide recommendations to NCC Security, as appropriate, to improve EPA's security posture or address a specific situation/incident.
- Ensure the firewall systems are hardened, monitored, and maintained so as to provide protection against malicious external threats through stateful inspection of network traffic to and from EPA's intranet, public access, demilitarized zone (DMZ), and Network Extension resources.

Security Technical Operations operates and manages multiple IDS/IPS sensors that are strategically placed to monitor and detect potentially malicious activity for the following

EPA traffic flows: Intranet, Region-to-Region, Internet entry, DMZ, Network Extension, and COOP/DR site. These systems provide real-time alerting for intrusions and incidents that occur within the monitored segments. The current effort also includes a contract with Internet Security Systems (ISS), on behalf of the EPA, to provide 24X7 monitoring of the Internet-facing IDS sensors in HQ and RTP. Uniformity in management and performance of the sensors is accomplished via documented procedures and processes that are kept current by the contractor.

Emerging and future requirements for **Security Technical Operations** include security configuration assessments, operations standards development and implementation, and security measurement and monitoring of technologies including virtualization, Web 2.0 collaboration suites, cloud computing, security zone definition and implementation within the NCC, and the implementation and use of sophisticated security, network, and server monitoring tools (e.g., BigFix, ArcSight security incident and event management [SIEM], Science Logic's EM7 tool, Symantec Endpoint Protection [SEP], etc.). Existing skills, experience, and capabilities in these emerging areas will be evaluated favorably.

Security Technical Operations operates the EPA SEIM tool (Arcsight) and coordinates with technology owners to gather log data. The CSIRC group will be the primary customer of the SEIM tool, but utilization by agency ISOs, SAs and NOSC is expected.

Security Technical Operations operates the EPA SNMP monitoring tool (EM7) from ScienceLogic. EM7 is used to monitor network devices (firewalls, IDS, routers, servers, etc…) and applications via SNMP. EM7 will also receive SNMP traps to alert on specific conditions. The NOSC will use EM7 as one of the key tools for situational awareness of EPA systems.

Security Technical Operations will support the NCC transition from perimeter firewall support to a security zone model that provides protection of the datacenter from the intranet. The new WAN2010 contract and Managed Trusted IP Services (MTIPS) security infrastructure will provide EPA perimeter security. The use of VMware within the NCC requires a new approach to security including the use of VM specific security (firewall, IDS, etc…) technology.

Security Technical Operations

- Design, installation, testing, configuration and operations/maintenance of the Cisco ISE, NCS and MSE into EPA's production network. Phase I support will focus on WLAN usage. Installation of the devices will be in RTP and DC.
- NSOC will produce documentation (SCD, Security Plan, SOP, etc…) for the NAC devices.
- NSOC will work with other groups and task orders for integration of directory authentication services into the NAC deployment.
- NSOC will assist identified task orders in verifying the WLAN Supplicant is FIPS compliant and all traffic from PC to back end WiSM2 device is encrypted with FIPS 140-2 level encryption. Use of NAC for end point control (desktop) will be considered a phase II (FY14) item.

- NSOC will assist identified task orders in creation and review of Windows Supplicant for WLAN Type 1(GFE), 2(EPA BYOD), 3(Guest) users.
- Provide and support NATing on RTP and DC firewall(s) to support type 1, 2 and 3 WLAN users Internet access. Port starvation should be considered with migration to Office365. No more than 2000 private IPs per public NATed IP.
- NATing firewall data should be sent to Arcsight.
- EDSD will work with TISS to address monitoring of NAT data within Arcsight.
- Test NAT fail over between RTP to DC and DC to RTP.
- Work with NCC, AT&T and EDSD on QOS options for type 2 and 3 WLAN users. This requirement will need to consider impact of Office365 traffic and IPv6 on QOS settings.

Operations Security Program Management supports the development, review, and updating of system security plans, performs security analysis and provides recommendations for proposed Agency initiatives resulting in modifications to the infrastructure and/or EPA's security posture.

Operations Security Program Management also provides auditing for the Enterprise Server (IBM z/OS Mainframe) five times a day to detect and identify any unauthorized use of mainframe resources. These audits are also supported during EPA disaster recovery efforts. Recommendations are provided to NCC Security, as appropriate. Experience and expertise in using the Vanguard auditing tool and Resource Access Control Facility (RACF) controls is required to perform this function.

Operations Security Program Management administers a portion of EPA's monitoring and compliance initiative via BindView. BindView is used for compliance checking and quarterly Federal Information Security Management Act (FISMA) reporting for all Agency systems. NCC's portion is focused on the BindView tool for UNIX. BindView engineers maintain and create BindView policies in accordance with EPA policy and coordinate an exception process with NCC Security for approval by EPA's Technology & Information Security Staff (TISS). BindView engineers provide support and issue resolution for the BindView tool and coordinate with EPA's Distributed System Support (DSS) organization to periodically review Standard Configuration Documents (SCD) for changes to ensure that the BindView queries match these changes. BindView is scheduled for replacement in 2010, so this work function may encompass a very short period of time. BigFix will be utilized for compliance monitoring in FY2011.

Operations Security Program Management operates the EPA Vulnerability Management (VM) initiative using the McAfee Foundstone tool. EPA currently maintains 5,000 Foundstone licenses. VM functions currently include the following:

Technical Vulnerability Assessments (TVA)

- Perform vulnerability scans as directed by NCC Security.
- Submit results of scan to system administrator (SA) for port justification and review of vulnerabilities found.

- Assist System Administrators (SAs) with interpreting scan results and remediation efforts.
- Create final reports at completion of scan and submit to NCC Security.
- Perform monthly scans of firewall-related servers and graphical user interface (GUI) access desktops. Submit results to NCC Security.

Vulnerability Management Support.

- Perform monthly discovery scans for all Internet Protocol (IP)-reachable, network-attached devices and provide in a searchable inventory database (DB).
- Identify server operating systems (OSs) and perform monthly vulnerability scans on systems identified as running server OSs.
- Support and maintain the EPA-purchased VM infrastructure of servers, business process, knowledge base, and a website for VM customer support.
- Use Foundstone's Remediation Module to manage the remediation of Agency servers in concert with responsible system administrators and Information Security Officers (ISOs).
- Produce a Vulnerability Management Dashboard and routine reports reflecting Agency-wide remediation activity by office/region on a monthly basis. Roll-up shall be by OS, site/location/organization, level of risk, etc.
- Support EPA's TISS/Technical Vulnerability Assessment Lab (TVAL) per established Memorandum of Understanding (MOU) agreement. A copy of the MOU is provided in the Technical Reference Library provided for this TO.
- Maintain VM documentation (e.g., processes, statements of work [SOWs], system documentation, etc.).
- Conduct data backups of VM devices as needed.

The Foundstone tool is scheduled for replacement during the first quarter of 2011. Following this replacement, vulnerability management support functions may be eliminated or redefined under this task.

Similar to the WAN Telecommunications Operations transition under the WAN2010 contract, EPA expects its security infrastructure operations to transition as well. WAN2010 will deliver the Federally-mandated Managed Trusted Internet Protocol Services (MTIPS), which will include the provisioning and management of all perimeter network security devices, including Internet-facing firewalls and sensors. Managed firewall services for non-Internet-facing devices will also be optionally available under WAN2010. However, currently, EPA expects all Intranet security operations and management to be supported by the TO.

3.1.1 WAN Operations Support

This task requires network operational support for the EPA WAN. Close coordination and assistance to the other tasks in this TO are required, especially with WAN Security Operations, which includes NETWORX MTIPS for the Agency Internet connection(s).

With the implementation of the WAN2010 effort and the award of the NETWORX contract, specification, procurement, implementation, configuration and management of WAN routers will not be within scope of this task. Close coordination with the NETWORX provider to properly specify, order, install, bring into and maintain in operational status WAN circuits and hardware is within scope, however. Any WAN circuits, hardware, software, maintenance, or support services necessary for WAN operations not procured through the NETWORX contract are within scope of this task. It is the goal of the task to keep the WAN operating as close to 100% availability as scheduled maintenance and budget allows. Support shall be provided at a base level with no additional cost to the EPA customer and at an elevated level with additional chargeback for network LAN support. Note that this task does not provide normal LAN operations. Support for the Washington D.C. Metropolitan Area Network is within scope as are operations of the network in the NCC. In addition to supporting large user populations, these two sites operate as the Agency's Internet gateways with the associated security infrastructure. In general, WAN servers shall be provisioned and operated by the ITS-EPA hosting task for use by telecom. This task shall provide WAN Domain Name Services, IP registrations and address management, WAN device access control (presently provided by TACACS+), Agency web proxy, caching and content filtering (presently provided by Blue Coat and Juniper appliances), WAN monitoring and reporting (presently provided by HPOV, TAVVE, Scrutinizer and other tools), and WAN diagnostics using network sniffers and similar tools.

All WAN equipment shall be operational 24 hours x 7 days per week to perform the prescribed support services. Hours for delivery of services are 06:30 A.M. - 8:00 P.M. Eastern Time. After hours pager support for network troubleshooting response is required. Some weekend or after-hours operations shall be required. Occasional travel to field sites for engineering, troubleshooting, and conference support shall be required. The task standard maintenance window is Wednesday nights, from 6 p.m. to 4:00 a.m. Eastern Time and 8 p.m. to midnight Eastern Time on the second Sunday of every month. Maintenance occurring outside these windows must be scheduled at least a week prior and approved by EPA. This policy excludes emergency maintenance. The contractor shall record all service requests in an approved tracking system that allows for escalation and workload reporting. The contractor shall respond to outages within 30 minutes. On-site response at NCC and DC, if required for repair, to non-business-hour outages will be within two hours of notification of an outage. The contractor shall track all open trouble tickets.

3.1.2 WAN Operations Tasks and Deliverables

Deliverables shall be provided electronically unless hard copies are requested. Network drawings are conducive to hard copy for increased clarity.

- Network Service Desk Function. Provide a single point of contact for network administrators. Facilitate network service restoration with minimal business impact within Service Level Agreements due to incidents. Provide TCO/TFN/SMA notifications shortly after each unscheduled outage or service degrading incident or prior to a scheduled outage via email.

- Network Incident Management. Provide normal service restoration as quickly as possible while minimizing adverse business operations impact. This responsibility includes escalation to higher level support group(s) as necessary. The responsibility includes logging, tracking, and managing the resolution to all WAN-related incidents, end-to-end, as well as handling and coordinating resolution of incidents related to external networks impacting the EPA. This responsibility includes identifying, resolving, and reporting security-related incidents. The contractor shall not allow any incident to go insufficiently resolved through lack of ownership or lack of coordination on the part of any member of the contractor's staff or any portion of the contractor's organization. This process also includes network Requests For Change (RFCs), currently provided under the Telecommunications Service Request (TSR) system. The RFC encompasses EPA IT customer requested moves, additions, and changes to the WAN including network project management and special projects to support evaluations, cross-task efforts, presentations, exercises and conferences. Provide and maintain all network documentation and procedures. Update documents as changes occur. All documentation shall be available in electronic format. The contractor shall review and correct all documentation for accuracy, grammar, spelling, and professional appearance, and deliver final versions in Agency standard formats and software. The intent is to create a logical, integrated, easily accessible repository for the task documentation of procedures, scripts, configurations, security changes, project history, and other WAN documentation. Sensitive task documentation shall be protected by appropriate security measures consistent with policy and data sensitivity. When directed by the task manager(s), the contractor shall incorporate specific documentation in EPA web site(s) in a timely manner. The contractor shall perform warehouse functions (including coordinating with EPA warehouse contractors) for items that affect the WAN task, including local and remote shipping and transportation associated with WAN equipment installations, spare parts replacement, normal and emergency equipment repair for all EPA WAN sites. TSR Reports with New/Pending status shall be available on-line shortly after TSRs are received, and shall be updated as changes occur. TSR Review and Recommendations- Created as assigned through the TSR process. See accompanying Technical Reference Library CD-ROM for TSR system report examples. A Technical Direction Status Report- Weekly shall be delivered: this report provides the weekly status of implementation of EPA technical direction to the support contractor.

- Network Problem Management. This responsibility includes identifying problems, reporting and tracking problems via the Remedy system, developing and providing the root cause analysis of incidents and initiating improvement or corrective actions to prevent incident recurrence. A Circuit Trouble Report - Status, trending, recommendations shall be delivered: this report provides the weekly status of circuit issues. A Root Cause Analysis Report shall be delivered: this report provides

recommendations for corrective actions for each significant network problem within one month.

- Network Configuration Management. This responsibility includes accounting for all network assets and configurations. Provide and maintain documentation of network assets and configurations, including security configurations. An example is the WAN Security Plan. Provide WAN hardware and software inventory and network hardware configurations. Coordinate EPA property and loaner equipment movement with the task manager(s), EPA property office(s), and support contractor(s) and contractor(s) (including maintenance providers) property offices so that the proper groups are notified and property is properly accounted for. The contractor shall maintain historical property information and otherwise assist EPA in locating EPA equipment including physical inventories of WAN tools, equipment, and software. Provide or provide input to a central Configuration Management Database/System and Definitive Software Library. Properly secure, control and maintain network software. Provide updates as changes occur, preferably automatically. WAN drawings shall be updated as changes occur. Hard copies shall be produced and delivered upon request. Periodic inventory reconciliations and reports to auditors shall be produced and delivered as requested. An example is the annual network hardware inventory audit.

- Network Change Management. Manage the network additions, modifications, or removals of WAN hardware, software, or circuits. Participate in Change Advisory Board (CAB) and engineering review boards governing network changes. Produce or provide input to a Forward Schedule of Change(s) (FAC). Input changes according to EPA guidelines in the EPA system for Change management, presently the Remedy system. Provide or participate in Post Implementation Reviews (PIR) to ensure the change met objectives, caused no unanticipated negative consequences and to solicit effected parties' feedback to monitor the effect of the change. Manage RFCs using industry standard project management professional (PMP) principles, guidelines and rigor. Ensure change back out plans are provided, tested, and approved prior to scheduled changes. A Task manager weekly report of network changes for previous weeks' changes shall be prepared and delivered. A Monthly report of network changes for previous month shall be prepared and delivered within 10 business days of month end. This report shall include PIR results and recommendations for improvement. Reports to include statistics including number of emergency changes shall be prepared and delivered on request. Focus shall be on reducing the number of emergency changes. The contractor shall provide email notification to the Task Manager of pending scheduled changes at risk due to incomplete approval and which approvers/areas are lacking.

- Network Service Level Management. Monitor and report on Service Level Agreement (SLA) performance monthly with service providers, such as the WAN 2010 NETWORX provider. Monitor and report on all WAN performance metrics to continuously improve network performance. Project bandwidth trends and report same monthly with previous month's data included with recommendations for WAN changes. Research, review, analyze, recommend and initiate RFCs for network changes to improve performance. Provide documentation of these activities, including information

papers, decision/recommendation papers, and project plans. The Quality Technology Subcommittee (QTS) Report of WAN circuit performance shall be provided monthly on the fifth business day of the new month for the previous month's performance. (A sample of this report is included in the Technical Reference Library)

- Network Security Management. Respond to security audits and required Automated Security Self-Evaluation and Remediation Tracking (ASSERT) database updates, as required. Support EPA development and maintenance of the WAN Security Plan which documents processes, procedures, architecture, interdependencies, and assumptions by which the EPA WAN implements, tests, and complies with governing federal security standards such as under the latest version of the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Recommended Security Controls for Federal Information Systems and Organizations.
- Network Business Management. Procurement of hardware, software, maintenance, circuits, and services as directed by EPA. Maintain network maintenance contract records including costs. Ensure that maintenance is in place, upon expiration of warranty for new systems, software, and hardware (except "as is" property) that support the task. Advise the task manager(s) 90 days prior to expiration so that sufficient time is available and arrangements may be made to cover the equipment or software with the appropriate maintenance contract. Advise the EPA task manager(s) when covered items may be safely removed from maintenance and periodically review, in coordination with the task manager(s) maintenance coverage to reduce maintenance costs. Ensure that maintenance contracts are revised in a timely fashion to account for items swapped out under maintenance contract so that the old item is removed and the new item is included under maintenance and there is no double coverage of old and new or lapse in coverage. Feed information to RFCs for cost analysis/impact of proposed RFC. Maintain WAN circuit listing including associated network costs, and update as changes occur. Cost listing should provide meaningful statistics including, but not limited to, the following: identify the last time the circuit was billed and paid as well as an outstanding balance; account summary for each circuit and how many months the billing is in arrears as of the end of the current month. Maintain monthly WAN circuit outage credit report including monetary credits for circuit outages and missed SLAs. Provide monthly hardware and software maintenance summary report. Provide monthly circuit invoice status report to ensure invoices are paid within government prompt payment guidelines and to prevent accrual of late payment charges and large invoice balances.

3.1.3 WAN Operations Schedule of Deliverables

DESCRIPTION	FREQUENCY	MEDIA	DISTRIBUTION
NOSC Project Plan	One-time delivery (Date of award + 30 days)	Hardcopy (2), Electronic attachment via Email	CO, TOCOR

TCO/TFN/SMA Notifications	Within 30 minutes (prime shift) and within one (1) hour (non-prime shift) of unscheduled events; Within two (2) days of scheduled events	Email	TOCOR
TSR Receipt Acknowledgement	Within one (1) business day of receipt	Email	TOCOR, TSR Originator
Technical Direction Status Report	Weekly	Email	TOCOR
Circuit Trouble Report	Weekly	Email	TOCOR
Root Cause Analysis Report	Within seven (7) days of event (Page 24 says 1 month – please make sure they are consistent)	Electronic attachment via Email	TOCOR
Task Manager Weekly Report	Weekly	Email	TOCOR
Network Changes Report	Monthly	Electronic attachment via Email	TOCOR
Emergency Changes Report	Ad hoc on request	Email	TOCOR
Scheduled Changes At Risk Report	As dictated by status	Email	TOCOR
SLA Performance Report	Monthly	Electronic attachment via Email	CO, TOCOR
QTS WAN Performance Report	Monthly by the fifth business day	Electronic attachment via Email	TOCOR
Hardware/Software Maintenance Report	Monthly	Electronic attachment via Email	TOCOR

3.1.4 WAN Operations Applicable Documents

Documents and information that may be useful to contractors for defining, scoping, and pricing proposals are provided in the accompanying Technical Reference Library CD-ROM.

3.1.5 WAN Operations Acceptance Criteria

Desired Outputs	Required Services	Performance Indicator	Monitoring Method	Incentives Positive & Negative
EPA is notified of WAN outages in a timely manner	**Contractor shall produce WAN outage notifications of the time in a timely manner**	**Notification is made within 30 minutes, 99.5% of the time during normal working hours and 99.5% of the time within 1 hour after normal working hours**	**Compare system time stamp of outage to Telecom Critical Outage notification email time stamp.**	When performance is above the standard, 10% of the Value specifie for this SLA will be awarded the contractor, pe contract quarter. When performance is below the standard, 25% of the Valu specified for this SLA will be assessed against th contractor, per contract quarter. These conditions apply to all events occurri during the measurement period (i.e., not singular events). *See Note Below*

EPA is notified of scheduled outages of the WAN	**Contractor shall notify EPA of all scheduled outages of the WAN with complete reports which shall contain, but not be limited to, such items as: date and time of outage; updates as restoration progresses; date and time the network was back online and operational; explanation of problem; an explanation of the impact of the outage on end uses; a list of impacted organizations; and, steps taken to restore to the pre-outage state**	**99.5% of the time within 2 days in advance of scheduled outage**	**Compare email time stamp of notification to the actual outage date.**	When performance is abo the standard, 10% of the Value specified for this SLA will be awarded the contractor, per contract quarter. When performan is below the standard, 25% of the Value specifie for this SLA will be assessed against the contractor, per contract quarter. These conditions apply to all events occurri during the measurement period (i.e., not singular events). *See Note Below*

Upon restoration of service, EPA receives a Root Cause Analysis (RCA) of outage and/or disruption of service.	**Contractor shall provide a Root Cause Analysis report when directed by EPA for large impact outages**	**98% of the time within 7 days of notification by EPA of need**	**Time differential between time stamp of written notification of need and time stamp of actual delivery. Recommended method of delivery for notification and report is via Notes mail.**	When performance is abo the standard, 10% of the Value specified for this SI will be awarded the contractor, per contract quarter. When performan is below the standard, 25% of the Value specifie for this SLA will be assessed against the contractor, per contract quarter. These conditions apply to all events occurri during the measurement period (i.e., not singular events). *See Note Below*
TSRs will be installed within the EPA-specified time frames	**The Contractor shall meet the specified installation commitments for the various TSR complexity categories 99.5% of the time**	**Complexity 1 with an installation commitment of 30 days including central rapid application deployment with an installation commitment of 3 business days; Complexity 2 with an installation commitment of 60-90 days; and, Complexity 3 with an installation commitment of 90-120 days**	**Time stamp comparison of TSR receipt email notifications to completion dates.**	When performance is abo the standard, 10% of the Value specified for this SI will be awarded the contractor, per contract quarter. When performan is below the standard, 25% of the Value specified for this SLA will be assessed against the contractor, per contract quarter. These conditions apply to all events occurring during the measurement period (i.e., not singular events). *See Note Below*

Network Performance	**The Contractor shall maintain the NCC production network**	**99.9% availability excluding scheduled and approved outages**	**Comparison and difference of total potential availability less scheduled and approved outages minus actual unapproved outage total time rendered into a percentage of actual availability.**	When performance is abo the standard, 10% of the Value specified for this SI will be awarded the contractor, per contract quarter. When performan is below the standard, 25% of the Value specified for this SLA will be assessed against the contractor, per contract quarter. These conditions apply to all events occurring during th measurement period (i.e., not singular events). *See Note Below*

NOTE: Each quarter's incentive, positive or negative will be accumulated in a pool. At the end of the contract year, this pool will be assessed and if the amount in the pool is positive, the contractor will be paid the accumulated pool amount. If the amount is negative, the negative amount in the pool will be withheld in a subsequent voucher.

Value = 1% of the labor costs for subtask 3.1, not to exceed the following amounts per year:

$9,528.59 Base Period
$20,767.87 Option Period I
$21,287.05 Option Period II
$21,819.83 Option Period III
$22,365.12 Option Period IV
$22,924.25 Option Period V

DESIRED OUTPUT	REQUIRED SERVICE	PERFORMANCE INDICATOR
Inventory is accurate at all times	The contractor shall maintain inventory and make updates as changes occur	100% accuracy
Documentation must be accurate, concise, error-free, professional and timely	The contractor shall provide accurate, concise, error-free, professional, and timely documentation 100% of the time and according to specified	100% accuracy

	delivery schedules. Some content leeway will be allowed for unscheduled outage reports generated in midst of service restoration	
Configuration changes must be processed through the change control systems before implementation.	The contract shall process all configuration changes through the change control system before implementation. Configuration changes spawned by unscheduled outages will be documented within the change control system as soon as time allows without negatively impacting service restoration.	100% compliance

3.2 National Computer Center (NCC) Security Management

3.2.1 NCC Security Management Support

Security Technical Operations involves the daily operations, maintenance, and administration of all security infrastructure devices used to protect and defend Agency IT resources and data. These devices include, but are not limited to, network monitoring appliances; host monitoring appliances; intrusion detection/prevention sensors, their placement, and their controls; and firewalls. Continuous monitoring and analyses of the data observed and reported by these components is also a routine requirement. Security Technical Operations adheres to, and ensures compliance with, all Agency technology standards for configurations, and is responsible for all operations procedures and documentation. Engineering support from the technical operations team is required whenever device testing and/or infrastructure changes are necessitated. The NCC currently operates all security infrastructure devices for protecting the Agency centralized computing resources and the WAN, including perimeter devices separating the EPA domain from the Internet, firewalls and sensors protecting public-facing IT resources in a de-militarized zone (DMZ), and firewalls and sensors protecting EPA's more sensitive Intranet resources. The Federal directives from the Office of Management and Budget for Trusted Internet Connections (TIC) and the inclusion of Managed Trusted Internet Protocol Services (MTIPS) within the scope of EPA's WAN2010 contract will likely result in a new distribution of security technical operations responsibilities. Until clarity in both Federal mandates and contract provisions is available, EPA will sub-divide Security Technical Operations support into two parts. Intranet Security Technical Operations will provide support for all devices related to protecting and defending EPA's more sensitive Intranet resources. Internet/Extranet Security Technical Operations will provide support for all devices related to

protecting and defending EPA's perimeter and DMZ resources. Operations support for some or all of the Internet/Extranet devices may shift to WAN2010 MTIPS over time. Operations support for Intranet devices may also change as a consequence of more stringent EPA security requirements than those supported by more generic MTIPS controls.

Operations Security Program Management provides the oversight, analyses, assessment and implications, documentation, recommendations, consulting, and reporting support to NCC Security Management. Security Change Management assesses, recommends, implements, and documents all potential changes to EPA's security infrastructure. Security Access Management considers the security implications and connectivity alternatives available for supporting NCC and WAN customers. Security Infrastructure Assessment and Planning provides strategic analyses and vision for Agency security needs compared to emerging technologies and the need for operations changes. Security consulting services to NCC customers may also be a part of this support. Lastly, Security Compliance Assessment and Reporting provides regular, recurring monitoring and analyses to ensure compliance of Agency IT resources with both Agency and Federal IT Security requirements; performs regular, recurring compliance monitoring and reporting; and supports special assessment projects that include, but are not limited to, Office of Inspectors General (OIG) audits/reviews, other oversight requirements from both internal EPA offices and external entities; risk assessment support for the NCC and WAN environments; and certification and accreditation support in accordance with Federal Information Security Management Act (FISMA) requirements.

3.2.2 NCC Security Management Tasks and Deliverables

Deliverables are to be provided electronically unless hard copies are requested. Security infrastructure drawings are conducive to hard copy for increased clarity.

Intranet Security. The contractor shall provide the technical implementation and operations support for the hardware and software security components of the Agency's security infrastructure for Intranet security. These components include, but are not limited to, network monitoring appliances (e.g., RealSecure); Network Access Control (NAC); host monitoring appliances for NCC's Intranet devices (e.g., Bindview); intrusion detection sensors, their placement, and controls; firewall administration (i.e., the main Agency Checkpoint firewall (AGF)); and, technical leadership in the evaluation and decisions regarding distributed network security appliances. The contractor shall provide all labor and supervision to provide operations and system maintenance for dedicated security servers and security software as identified by the Agency through written technical direction. Included in the implementation of operation and maintenance activities for new technologies is the development of installation instructions, operational security procedures, and other appropriate documentation. The contractor shall serve as the System Administrator (SA) for dedicated production security servers. The contractor shall ensure compliance with NCC operations and security directives.

Internet Security. Until the Agency transitions its Internet connectivity and security to its WAN2010 managed services under MTIPS, the contractor supporting this TO shall provide the

technical implementation and operations support for the hardware and software security components of the Agency's security infrastructure for Internet security. These components include, but are not limited to, network monitoring appliances (e.g., RealSecure); host monitoring appliances for NCC's DMZ devices (e.g., Bindview); intrusion detection sensors, their placement, and controls; and, firewall administration (i.e., the Agency DMZ Checkpoint firewall (PA)). The contractor shall provide all labor and supervision to provide the operations and system maintenance for dedicated security servers and security software as identified by the Agency through written technical direction. Included in the implementation of operation and maintenance activities for new technologies is the development of installation instructions, operational security procedures, and other appropriate documentation. The contractor shall serve as the SA for dedicated production security servers. The contractor shall ensure compliance with NCC operations and security directives. Following the transition to MTIPS, the contractor supporting this TO shall primarily focus on Intranet security (described above), but shall continue to be responsible for collaboration, communication, consultation, and analyses with the WAN2010 MTIPS contractor as necessary to monitor, trouble-shoot, investigate, and/or mitigate technical problems, issues, and/or incidents related to Internet connectivity. These levels of support are required to be normal operations practices and procedures of the EPA NOSC.

For both **Intranet Security** and **Internet Security** operations, the contractor shall:

--operate and maintain all security infrastructure devices identified by EPA under the scope of this task order at the specified service level. The contractor shall measure and report availability for each device as:

> Availability = 100 % uptime / (uptime + downtime), where downtime does not include regularly scheduled maintenance time nor EPA-approved emergency maintenance time. Device availability reports shall be produced monthly as part of an SLA Performance Report.

--provide 24X7 on-call support to resolve issues with security infrastructure devices.
--review and monitor security infrastructure device logs daily and act on all identified issues.
--review and monitor firewall logs daily to identify trends and assist incident response activities.
--perform specialized and general system maintenance, including patching, user access, and contractor interfaces.
--develop, maintain, and document various scripts for security infrastructure devices and support systems, including monitoring, integrity checking, log rotation and retention, operating system maintenance, and statistics/trending.
--support, identify, and plan various security system backup methods and operations.
--test and patch production operating systems and applications as determined by software contractors and/or alerts from Government or commercial sources.
--update documentation for system administration, troubleshooting, GUI access procedures as needed.
--coordinate with all other NCC operations components as needed for problem and incident resolution.

--provide support and maintenance for firewall logs/archival. Respond to ad hoc requests for log data.
--implement root/administrator access restriction to a known set of support personnel.
--ensure that access to system-level files and services is restricted by use of operating system level file permissions. The contractor shall maintain a database listing users, their access and permissions, their roles, and security level.
--use Agency standard configurations for all security infrastructure devices as available.

Security Engineering. The contractor shall provide engineering support for the configuration, management, audit, and operation of EPA's security infrastructure components, including, but not limited to, firewalls, IDS/IPS, authentication servers, virtual private networks (VPNs), Network Access Control (NAC) and server assessment tools. The contractor shall provide engineering support for security pilots, technology testing/product assessments, and standards development. A security test-lab environment shall be established for purposes of testing the effects and implications of security infrastructure changes, including, but not limited to, hardware and software changes, firewall rule changes, script changes, scanning and monitoring procedures and parameter changes.

Security Change Management. The contractor shall utilize an automated Change Management process to identify, schedule, notify, and implement changes to all major operating environments at NCC managed data center(s). Specific EPA managers as well as contractor groups are required to review and approve/disapprove changes as submitted to the Change Management process. This task requires attendance by the contractor to all Change Management meetings as well as approving all change requests. For NCC Security Management, change management includes, but is not limited to, required and/or proposed changes to system configurations, and required and/or proposed changes to system security controls. Due to data sensitivity, the NCC Firewall Rule Request (FRR) process operates independently from the normal operations change management process. The contractor shall manage the FRR workflow, coordinating meetings and FRR development between the various stakeholders, and ensuring sufficient documentation is present to justify the change. The contractor shall work with customers to develop FRR documentation. While the majority of FRRs will be related to NCC Application Deployment Checklist (ADC) application, the contractor shall also help create FRRs for other customers.

Security Access Management. The contractor shall develop, manage, and oversee a security access management process for requests and requirements from the Internet and/or Intranet, as well as among diverse security zones within the NCC. The contractor shall be responsible for utilizing Agency approved security controls and monitoring software tools to perform daily auditing of security infrastructure system and system file access attempts; failed logon attempts, repeated password changes, attempts to modify or alter the contents or protection of system files, changes to system exits, started tasks and Program Properties tables.

Security Assessment and Planning. The contractor shall conduct regular recurring vulnerability scanning of IP-reachable network-attached devices within the EPA Intranet (up to the licensing limits of the vulnerability toolset), review NCC's general support systems (GSSs)

and major application (MA) security plans, review security plans required and prepared as par of the Application Deployment Checklist (ADC) workflow process as described in the Custom Applications Management task order under the ITS-EPA II BPA, and evaluate new and emerging security technologies to identify security risks and impacts to the NCC operations environment. Identified vulnerabilities must be verified, documented, and remediated within Agency-prescribed processes and schedule. Security plans must be checked for compliance with the National Institute and Standards (NIST) 800-18, Guide for Developing Security Plans for Federal Information Systems, guidelines and for technical content appropriateness. The contractor shall coordinate with the GSS and MA system owners to ensure that all technical security controls have been tested and perform as required. The contractor shall ensure that documentation is maintained to show evidence of the implementation and successful operation of all technical security controls. The contractor may also provide security assessment and planning consulting services on demand to EPA customers of the NCC, under the direction and involvement of the TOCOR. These services may take the form of security plan reviews and assessments, security architecture advice, and/or security incident mitigation strategies. Security technologies for evaluation shall be indentified by and/or approved by the task manager through written technical direction. Reports shall be generated and presented to the task manager in NCC approved formats for either informational purposes or in support of NCC decisions on security technology strategic direction.

Security Compliance Assessment and Reporting. The contractor shall manage compliance checking and quarterly Federal Information Security Management Act (FISMA) reporting for Agency general support systems (GSSs). This effort includes the execution of approved Agency compliance tools on a regularly defined schedule; review and assessment of compliance results against approved system configuration and security control policies and procedures; management and oversight of all remediation activities; and the preparation of quarterly reports documenting NCC GSS compliance. Ad hoc compliance testing, assessment, remediation, and reporting are also required as dictated by emergency situations, such as critical system patches and/or system security control changes due to imminent threats. The contractor shall support and participate in external oversight audits as needed, ensuring inquiries and responses are coordinated, documented, and reviewed by the NCC.

3.2.3 NCC Security Management Schedule of Deliverables

DESCRIPTION	FREQUENCY	MEDIA	DISTRIBUTION
NOSC Project Plan	One-time delivery (Date of award + 30 days)	Hardcopy (2), Electronic attachment via Email	CO, TOCOR
Technical Direction Status Report	Weekly	Email	TOCOR

Task Manager Weekly Report	Weekly	Email	TOCOR
SLA Performance Report	Monthly	Electronic attachment via Email	CO, TOCOR
NCC GSS Compliance Report	Quarterly by the fifth business day	Electronic attachment via Email	TOCOR, NCC ISO
Server Policy Compliance Report	Monthly	Electronic attachment via Email	TOCOR, NCC ISO
Vulnerability Assessment Report	Monthly	Electronic attachment via Email	TOCOR. NCC ISO
GSS/MA Security Plan Assessment	Receipt of plan for review + 5 business days	Email	TOCOR, NCC ISO, System/application owner
Firewall Rule Request Status Report	Weekly	Electronic attachment via Email	TOCOR
Emerging Security Technology Review	Bi-annual	Technical Briefing	TOCOR, NCC/SBMB
Open Security Issues Status Report	Monthly	Email	TOCOR, NCC ISO
Security Access Report	Quarterly by the fifth business day	Electronic attachment via Email	TOCOR, NCC ISO

3.2.4 NCC Security Management Applicable Documents

Documents and information that may be useful to contractors for defining, scoping, and pricing proposals are provided in the accompanying Technical Reference Library CD-ROM.

3.2.5 NCC Security Management Acceptance Criteria

Desired Outputs	Required Services	Performance Indicator	Monitoring Method	Incentives Positive & Negative
All security infrastructure components will be available and operational	**The Contractor shall maintain and operate all security infrastructure components under its management control at a minimum availability and operating status, during the Agency's 24 X 7 operations schedule (excepting the regular, recurring weekly systems maintenance window and/or any emergency scheduled maintenance windows declared by EPA)**	**99.9% of the time**	**Task Manager review of monthly SLA report.**	When performance is abov the standard, 10% of the Value specified for thi SLA will be awarded the contractor, per contract quarter. When performance is below the standard, 25% of the Value specified for thi SLA will be assessed against the contractor, per contract quarter. These conditions apply to all components under operation and maintenance during the measurement period (i.e., n singular components). *See Note Below*
Severity 1 security incidents shall be escalated in a timely manner	**The contractor shall escalate all severity 1 incidents within 30 minutes**	**99.5% of the time**	**Task Manager review of monthly**	When performance is abov the standard, 10% of the Value specified for this SL will be awarded the contractor, per contract quarter. When performanc is below the standard, 25% of the Value specified for t SLA will be assessed again the contractor, per contract quarter. These conditions apply to all events occurrin during the measurement period (i.e., not singular events). *See Note Below*

All security infrastructure components are maintained and operated so that compliance with Agency policies and standards are maintained, there are no customer service disruptions, or reduced availability	**The Contractor shall maintain and operate all security infrastructure components under its management contract such that security incidents do not result in customer services disruptions or reduced availability**	**Less than 1% of all security incidents result in customer service disruptions or reduced availability**		When performance is abov the standard, 10% of the Value specified for this SL. will be awarded the contractor, per contract quarter. When performanc is below the standard, 25% of the Value specified for tl SLA will be assessed again the contractor, per contract quarter. These conditions apply to all components under operation and maintenance during the measurement period (i.e., n singular components). *See Note Below*

NOTE: Each quarter's incentive, positive or negative will be accumulated in a pool. At the end of the contract year, this pool will be assessed and if the amount in the pool is positive, the contractor will be paid the accumulated pool amount. If the amount is negative, the negative amount in the pool will be withheld in a subsequent voucher.

Value = 1% of the labor costs for subtask 3.2, not to exceed the following amounts per year:

$15,135.70 Base Period
$31,982.09 Option Period I
$32,781.36 Option Period II
$33,601.11 Option Period III
$34,440.91 Option Period IV
$35,301.88 Option Period V

Value = 2% of the labor costs for subtask 3.2, not to exceed the following amounts per year:

$30,271.39 Base Period
$63,964.18 Option Period I
$65,562.72 Option Period II
$67,202.22 Option Period III
$68,881.81 Option Period IV
$70,603.75 Option Period V

DESIRED OUTPUT	REQUIRED SERVICE	PERFORMANCE INDICATOR
All security infrastructure components are maintained at EP's "green" patch level status	The contractor shall maintain all security infrastructure components under its management control at EPA's "green" patch level status consistently from month to month. "Green" patch level status means that 90% or more cumulative patches and updates have been installed	100%
Little or no re-submittal for all Firewall Rule Requests and there are little or no failure results for all firewall rule implementations.	The Contractor shall maintain a 5% or less re-submittal result for all Firewall Rule Requests and shall maintain 5% or less failure results fro all firewall rule implementation.	100% of the time

4. GENERAL BUSINESS REQUIREMENTS AND OBJECTIVES

The contractor must adhere to all applicable EPA, OEI, OTOP, NCC, and Agency Working Capital Fund (WCF) policies, procedures, directives, and standards.

4.1 Interfaces/Communication

Coordination and communication across tasks and separate task orders is paramount. Interfaces include, but are not limited to, the NCC Management, NCC Deployment Team, NCC Hosting Team, NCC Security Team, Business Intelligence and Analytics Center (BIAC), Customers, Contractors, Agency Teams, and other technology experts required to deliver the services specified in the task/task order. The contractor shall continuously coordinate and communicate across tasks, task orders, and, when necessary, other contracts, including ITS-EPA, ITS-BISS, and WAN2010.

The contractor will also use OTOP's Management Information Center (OMIC) for task/work assignments and contract deliverables and eBusiness for Working Capital Fund order

processing, reporting, workload and other requirements, as needed.

Revised 4/23/13

Attachment #3 CLINs

Base Period 04/01/2011-09/30/2011

CLINs	Labor Category	Task Order Rate	Quantity	Total
0001	Sr. Project Director Level II	$		$
0002	Sr. Project Director Level I	$		$
0003	Sr. Technologist	$		$
0004	Sr. Functional Expert	$		$
0005	Project Manager	$		$
0006	Technical Expert	$		$
0007	Functional Expert	$		$
0008	Application Development Team Leader	$		$
0009	Systems Integration Engineer	$		$
0010	Technical Specialist	$		$
0011	Sr. Business Systems Consultant	$		$
0012	Sr. Client/Server Developer	$		$
0013	Business Systems Analyst	$		$
0014	Training Specialist	$		$
0015	Sr. Systems Programmer	$		$
0016	Systems Programmer	$		$
0017	Analyst/Programmer	$		$
0018	Documentation Specialist	$		$
0019	Research Analyst	$		$
0020	Project Administration Staff	$		$
0021	I&A Operational Support Technician III	$		$
0022	I&A Operational Support Technician II	$		$
0023	I&A Operational Support Technician I	$		$
0024	Application Developer III	$		$
0025	Application Developer II	$		$
0026	Application Developer I	$		$
0027	Application Analyst III	$		$
0028	Application Analyst II	$		$
0029	Application Analyst I	$		$
0030	Database Administrator	$		$
0031	Application Operator II	$		$
0032	Application Operator I	$		$
0033	Help Desk Manager	$		$
0034	Help Desk III	$		$
0035	Help Desk II	$		$
0036	Help Desk I	$		$
	Subtotal Labor Costs			
0037	Open Market ODCs			$
0038	[redacted] G&A on open market ODCs			$
0039	GSA ODCs			$
0040	[redacted] Sub Handling Fee on CTA ODCs			$
	Total ODCs*			$

	Total (Labor and ODCs)	**$ 3,315,270.15**
0041	**Firm Fixed Price CLIN for CTA Shut down support**	[redacted]

Option Period 1 10/01/2011-09/30/2012

CLIN		Task Order Rate	Quanity	Total
1001	Sr. Project Director Level II-onsite	$	[redacted]	$
1001a	Sr. Project Director Level II-Cont. site	$		
1002	Sr. Project Director Level I-onsite	$		$
1002a	Sr. Project Director Level I-Cont.site	$		
1003	Sr. Technologist-Onsite	$		$
1003a	Sr. Technologist-Cont. site	$		
1004	Sr. Functional Expert-Onsite	$		$
1004a	Sr. Functional Expert-Cont. site	$		
1005	Project Manager-Onsite	$		
1005a	Project Manager-Cont.site	$		$
1006	Technical Expert-Onsite	$		$
1006a	Technical Expert-Cont. site	$		$
1007	Functional Expert-Onsite	$		$
1007a	Functional Expert-Cont.site	$		
1008	App.Develop.Team Leader-Onsite	$		$
1008a	App.Develop.Team Leader-Cont. site	$		
1009	Sy. Integration Eng-Onsite	$		$
1009a	Sy. Integration Eng-Cont. site	$		
1010	Technical Specialist-Onsite	$		$
1010a	Technical Specialist-Cont.site	$		$
1011	Sr. Business Systems Consultant-Onsite	$		$
1011a	Sr. Business Systems Consultant-Cont. site	$		
1012	Sr. Client/Server Developer-Onsite	$		$
1012a	Sr. Client/Server Developer-Cont.site	$		
1013	Business Systems Analyst-Onsite	$		$
1013a	Business Systems Analyst-Cont. site	$		
1014	Training Specialist-Onsite	$		$
1014a	Training Specialist-Cont. site	$		
1015	Sr. Systems Programmer-Onsite	$		$
1015a	Sr. Systems Programmer-Cont. site	$		
1016	Systems Programmer-Onsite	$		
1016a	Systems Programmer-Cont. site	$		
1017	Analyst/Programmer-Onsite	$		
1017a	Analyst/Programmer-Cont. site	$		
1018	Documentation Specialist-Onsite	$		$
1018a	Documentation Specialist-Cont. site	$		
1019	Research Analyst-Onsite	$		$
1019a	Research Analyst-Cont.site	$		
1020	Project Administration Staff-Onsite	$		
1020a	Project Administration Staff-Cont. site	$		

1021	I&A Oper.Support Tech III-Onsite	$	[redacted]	[redacted]	[redacted]
1021a	I&A Oper.Support Tech III-Cont. site	$			
1022	I&A Oper. Support Tech II-Onsite	$			
1022a	I&A Oper. Support Tech II-Cont. site	$			
1023	I&A Oper. Support Tech I-Onsite	$			
1023a	I&A Oper. Support Tech I-Cont. site	$			
1024	Application Developer III-Onsite	$			
1024a	Application Developer III-Cont. site	$			
1025	Application Developer II-Onsite	$			
1025a	Application Developer II-Cont. site	$			
1026	Application Developer I-Onsite	$			
1026a	Application Developer I-Cont. site	$			
1027	Application Analyst III-Onsite	$			
1027a	Application Analyst III-Cont. site	$			
1028	Application Analyst II-Onsite	$			
1028a	Application Analyst II-Cont. site	$			
1029	Application Analyst I-Onsite	$			
1029a	Application Analyst I-Cont. site	$			
1030	Database Administrator-Onsite	$			
1030a	Database Administrator-Cont. site	$			
1031	Application Operator II-Onsite	$			
1031a	Application Operator II-Cont. site	$			
1032	Application Operator I-Onsite	$			
1032a	Application Operator I-Cont. site	$			
1033	Help Desk Manager-Onsite	$			
1033a	Help Desk Manager-Cont. site	$			
1034	Help Desk III-Onsite	$			
1034a	Help Desk III-Cont. site	$			
1035	Help Desk II-Onsite	$			
1035a	Help Desk II-Cont. site	$			
1036	Help Desk I -Onsite	$			
1036a	Help Desk I -Cont. site	$			
1041	Systems Operator-Onsite	$			
1041a	Systems Operator-Cont site	$			
	Subtotal Labor Cost			[redacted]	$
1037	Open Market ODCs				$
1038	[redacted] G&A on open market ODCs				$
1039	GSA ODCs				$
1040	[redacted] Sub Handling Fee on CTA ODCs				$
	Total ODCs*				$
	Total (Labor and ODCs)				$ 6,612,086.79

Option Period 2 10/01/12-09/30/13

CLIN		Task Order Rate	Quanity	Total
2001	Sr. Project Director Level II-onsite	$		$
2001a	Sr. Project Director Level II-Cont site	$		
2002	Sr. Project Director Level I-onsite	$		$
2002a	Sr. Project Director Level I-Cont site	$		
2003	Sr. Technologist-onsite	$		$
2003a	Sr. Technologist-Cont site	$		
2004	Sr. Functional Expert-onsite	$		$
2004a	Sr. Functional Expert-Cont site	$		
2005	Project Manager-onsite	$		$
2005a	Project Manager-Cont site	$		
2006	Technical Expert-onsite	$		$
2006a	Technical Expert-Cont site	$		
2007	Functional Expert-onsite	$		$
2007a	Functional Expert-Cont site	$		
2008	App Devt Team Leader-onsite	$		$
2008a	App Devt Team Leader-Cont site	$		
2009	Syst Integ Engineer-onsite	$		$
2009a	Syst Integ Engineer-Cont site	$		
2010	Technical Specialist-onsite	$		$
2010a	Technical Specialist-Cont site	$		
2011	Sr. Bus Sys Consultant-onsite	$		$
2011a	Sr. Bus Sys Consultant-Cont site	$		
2012	Sr. Client/Server Developer-onsite	$		$
2012a	Sr. Client/Server Developer-Cont site	$		
2013	Business Systems Analyst-onsite	$		$
2013a	Business Systems Analyst-Cont site	$		
2014	Training Specialist-onsite	$		$
2014a	Training Specialist-Cont site	$		
2015	Sr. Systems Programmer-onsite	$		$
2015a	Sr. Systems Programmer-Cont site	$		
2016	Systems Programmer-onsite	$		$
2016a	Systems Programmer-Cont site	$		
2017	Analyst/Programmer-onsite	$		$
2017a	Analyst/Programmer- Cont site	$		
2018	Documentation Specialist-onsite	$		$
2018a	Documentation Specialist-Cont site	$		
2019	Research Analyst-onsite	$		$
2019a	Research Analyst-Cont site	$		
2020	Project Administration Staff-onsite	$		$
2020a	Project Administration Staff-Cont site	$		
2021	I&A Oper Support Tech III-onsite	$		$
2021a	I&A Oper Support Tech III-Cont site	$		
2022	I&A Oper Support Tech II-onsite	$		$
2022a	I&A Oper Support Tech II-Cont. site	$		
2023	I&A Oper Support Tech I-onsite	$		$

2023a	I&A Oper Support Tech I-Cont. site	$	[redacted]	$ [redacted]
2024	Application Developer III-onsite	$		$
2024a	Application Developer III-Cont site	$		
2025	Application Developer II-onsite	$		$
2025a	Application Developer II-Cont. site	$		
2026	Application Developer I-onsite	$		$
2026a	Application Developer I-Cont site	$		
2027	Application Analyst III-onsite	$		$
2027a	Application Analyst III-Cont site	$		
2028	Application Analyst II-onsite	$		$
2028a	Application Analyst II-Cont site	$		
2029	Application Analyst I-onsite	$		$
2029a	Application Analyst I-Cont site	$		
2030	Database Administrator-onsite	$		$
2030a	Database Administrator-Cont site	$		
2031	Application Operator II-onsite	$		$
2031a	Application Operator II-Cont site	$		
2032	Application Operator I-onsite	$		$
2032a	Application Operator I-Cont site	$		
2033	Help Desk Manager-onsite	$		$
2033a	Help Desk Manager-Cont site	$		
2034	Help Desk III-onsite	$		$
2034a	Help Desk III-Cont site	$		
2035	Help Desk II-onsite	$		$
2035a	Help Desk II-Cont site	$		
2036	Help Desk I -onsite	$		$
2036a	Help Desk I -Cont site	$		
2041	Systems Operator-Onsite	$		
2041a	Systems Operator-Cont site	$		
	Subtotal Labor Cost			$
2037	Open Market ODCs			$
2038	[redacted] G&A on open market ODCs			$
2039	GSA ODCs			$
2040	[redacted] ub Handling Fee on CTA ODCs			$
	Total ODCs*			$
	Total (Labor and ODCs)			$ [redacted]

Option Period 3 10/01/13-09/30/14

CLIN			Task Order Rate	Quanity	Total
3001	Sr. Project Director Level II-onsite	$	[redacted]	[redacted]	$ [redacted]
3001a	Sr. Project Director Level II-Cont site	$			
3002	Sr. Project Director Level I-onsite	$			
3002a	Sr. Project Director Level I-Cont site	$			
3003	Sr. Technologist-onsite	$			
3003a	Sr. Technologist-Cont site	$			

3004	Sr. Functional Expert-onsite	$	[redacted]	$	[redacted]
3004a	Sr. Functional Expert-Cont site	$		$	
3005	Project Manager-onsite	$		$	
3005a	Project Manager-Cont site	$		$	
3006	Technical Expert-onsite	$		$	
3006a	Technical Expert-Cont site	$		$	
3007	Functional Expert-onsite	$		$	
3007a	Functional Expert-Cont site	$		$	
3008	App Develop Team Leader-onsite	$		$	
3008a	App Develop Team Leader-Cont site	$		$	
3009	Sys Integration Engineer-onsite	$		$	
3009a	Sys Integration Engineer-Cont site	$		$	
3010	Technical Specialist-onsite	$		$	
3010a	Technical Specialist-Cont site	$		$	
3011	Sr. Bus Systems Consultant-onsite	$		$	
3011a	Sr. Bus Systems Consultant-Cont site	$		$	
3012	Sr. Client/Server Developer-onsite	$		$	
3012a	Sr. Client/Server Developer-Cont site	$		$	
3013	Business Systems Analyst-onsite	$		$	
3013a	Business Systems Analyst-Cont site	$		$	
3014	Training Specialist-onsite	$		$	
3014a	Training Specialist-Cont site	$		$	
3015	Sr. Systems Programmer-onsite	$		$	
3015a	Sr. Systems Programmer-Cont site	$		$	
3016	Systems Programmer-onsite	$		$	
3016a	Systems Programmer-Cont site	$		$	
3017	Analyst/Programmer-onsite	$		$	
3017a	Analyst/Programmer-Cont site	$		$	
3018	Documentation Specialist-onsite	$		$	
3018a	Documentation Specialist-Cont site	$		$	
3019	Research Analyst-onsite	$		$	
3019a	Research Analyst-Cont site	$		$	
3020	Project Administration Staff-onsite	$		$	
3020a	Project Administration Staff-Cont site	$		$	
3021	I&A Oper Support Tech III-onsite	$		$	
3021a	I&A Oper Support Tech III-Cont site	$		$	
3022	I&A Oper Support Tech II-onsite	$		$	
3022a	I&A Oper Support Tech II-Cont site	$		$	
3023	I&A Oper Support Tech I-onsite	$		$	
3023a	I&A Oper Support Tech I-Cont site	$		$	
3024	Application Developer III-onsite	$		$	
3024a	Application Developer III-Cont site	$		$	
3025	Application Developer II-onsite	$		$	
3025a	Application Developer II-Cont site	$		$	
3026	Application Developer I-onsite	$		$	
3026a	Application Developer I-Cont site	$		$	
3027	Application Analyst III-onsite	$		$	

3027a	Application Analyst III-onsite	$	[redacted]	$ [redacted]
3028	Application Analyst II-onsite	$		$
3028a	Application Analyst II-Cont site	$		
3029	Application Analyst I-onsite	$		$
3029a	Application Analyst I-Cont site	$		
3030	Database Administrator-onsite	$		$
3030a	Database Administrator-Cont site	$		
3031	Application Operator II-onsite	$		$
3031a	Application Operator II-Cont site	$		
3032	Application Operator I-onsite	$		$
3032a	Application Operator I-Cont site	$		
3033	Help Desk Manager-onsite	$		$
3033a	Help Desk Manager-Cont site	$		
3034	Help Desk III-onsite	$		$
3034a	Help Desk III-Cont site	$		
3035	Help Desk II-onsite	$		$
3035a	Help Desk II-Cont site	$		
3036	Help Desk I -onsite	$		$
3036a	Help Desk I -Cont site	$		
3041	Systems Operator-Onsite	$		
3041a	Systems Operator-Cont site	$		
	Subtotal Labor Cost		[redacted]	$
3037	Open Market ODCs			$
3038	[redacted] G&A on open market ODCs			$
3039	GSA ODCs			$
3040	[redacted] Sub Handling Fee on CTA ODCs			$
	Total ODCs*			$
	Total (Labor and ODCs)			$ 6,684,809.65

Option Period 4 10/01/14-09/30/15

CLIN			Task Order Rate	Quanity	Total
4001	Sr. Project Director Level II-onsite	$	[redacted]	[redacted]	[redacted]
4001a	Sr. Project Director Level II-Cont site	$			
4002	Sr. Project Director Level I-onsite	$			
4002a	Sr. Project Director Level I-Cont site	$			
4003	Sr. Technologist-onsite	$			
4003a	Sr. Technologist-Cont site	$			
4004	Sr. Functional Expert-onsite	$			
4004a	Sr. Functional Expert-Cont site	$			
4005	Project Manager-onsite	$			
4005a	Project Manager-Cont site	$			
4006	Technical Expert-onsite	$			
4006a	Technical Expert-Cont site	$			
4007	Functional Expert-onsite	$			

4007a	Functional Expert-Cont site	$	[redacted]	[redacted]	[redacted]
4008	App Develop Team Leader-onsite	$			
4008a	App Develop Team Leader-Cont site	$			
4009	Systems Integration Engineer-onsite	$			
4009a	Systems Integration Engineer-Cont site	$			
4010	Technical Specialist-onsite	$			
4010a	Technical Specialist-Cont site	$			
4011	Sr. Bus Systems Consultant-onsite	$			
4011a	Sr. Bus Systems Consultant-Cont site	$			
4012	Sr. Client/Server Developer-onsite	$			
4012a	Sr. Client/Server Developer-Cont site	$			
4013	Business Systems Analyst-onsite	$			
4013a	Business Systems Analyst-Cont site	$			
4014	Training Specialist-onsite	$			
4014a	Training Specialist-Cont site	$			
4015	Sr. Systems Programmer-onsite	$			
4015a	Sr. Systems Programmer-Cont site	$			
4016	Systems Programmer-onsite	$			
4016a	Systems Programmer-Cont site	$			
4017	Analyst/Programmer-onsite	$			
4017a	Analyst/Programmer-onsite	$			
4018	Documentation Specialist-onsite	$			
4018a	Documentation Specialist-Cont site	$			
4019	Research Analyst-onsite	$			
4019a	Research Analyst-onsite	$			
4020	Project Administration Staff-onsite	$			
4020a	Project Administration Staff-Cont site	$			
4021	I&A Oper Support Tech III-onsite	$			
4021a	I&A Oper Support Tech III-Cont site	$			
4022	I&A Oper Support Tech II-onsite	$			
4022a	I&A Oper Support Tech II-onsite	$			
4023	I&A Oper Support Tech I-onsite	$			
4023a	I&A Oper Support Tech I-Cont site	$			
4024	Application Developer III-onsite	$			
4024a	Application Developer III-Cont site	$			
4025	Application Developer II-onsite	$			
4025a	Application Developer II-Cont site	$			
4026	Application Developer I-onsite	$			
4026a	Application Developer I-Cont site	$			
4027	Application Analyst III-onsite	$			
4027a	Application Analyst III-Cont site	$			
4028	Application Analyst II-onsite	$			
4028a	Application Analyst II-Cont site	$			
4029	Application Analyst I-onsite	$			
4029a	Application Analyst I-Cont site	$			
4030	Database Administrator-onsite	$			
4030a	Database Administrator-Cont site	$			

4031	Application Operator II-onsite	$	[redacted]	$
4031a	Application Operator II-Cont site	$		
4032	Application Operator I-onsite	$		$
4032a	Application Operator I-Cont site	$		
4033	Help Desk Manager-onsite	$		$
4033a	Help Desk Manager-Cont site	$		
4034	Help Desk III-onsite	$		$
4034a	Help Desk III-Cont site	$		
4035	Help Desk II-onsite	$		$
4035a	Help Desk II-Cont site	$		
4036	Help Desk I -onsite	$		$
4036a	Help Desk I -Cont site	$		
4041	Systems Operator-Onsite	$		
4041a	Systems Operator-Cont site	$		
4042	Security Specialist-Onsite	$		
4042a	Security Specialist-Cont site	$		
4043	Systems Administrator-Onsite	$		
4043a	Systems Administrator-Cont. site	$		
4044	Storage Engineer-Onsite	$		
4044a	Storage Engineer-Cont site	$		
4045	Network Engineer-Onsite	$		
4045a	Network Engineer-Cont site	$		
4046	Infrastructure Architect-Onsite	$		
4046a	Infrastructure Architect-Cont site	$		
	Subtotal Labor Cost			$
4037	Open Market ODCs			$
4038	33.34% G&A on open market ODCs			$
4039	GSA ODCs			$
4040	1.83% Sub Handling Fee on CTA ODCs			$
	Total ODCs*			$
	Total (Labor and ODCs)			$ 6,566,400.98

Option Period 5 10/01/15-09/30/16

CLIN			Task Order Rate	Quanity	Total
5001	Sr. Project Director Level II-onsite	$	[redacted]	[redacted]	[redacted]
5001a	Sr. Project Director Level II-Cont site				
5002	Sr. Project Director Level I-onsite	$			
5002a	Sr. Project Director Level I-Cont site				
5003	Sr. Technologist-onsite	$			
5003a	Sr. Technologist-Cont site				
5004	Sr. Functional Expert-onsite	$			
5004a	Sr. Functional Expert-Cont site				
5005	Project Manager-onsite	$			
5005a	Project Manager-Cont site				
5006	Technical Expert-onsite	$			
5006a	Technical Expert-Cont site				

5007	Functional Expert-onsite	$	[redacted]	$	[redacted]
5007a	Functional Expert-Cont site				
5008	App Develop Team Leader-onsite	$		$	
5008a	App Develop Team Leader-Cont site				
5009	Syst Integration Engineer-onsite	$		$	
5009a	Syst Integration Engineer-Cont site				
5010	Technical Specialist-onsite	$		$	
5010a	Technical Specialist-Cont site				
5011	Sr. Bus Systems Consultant-onsite	$		$	
5011a	Sr. Bus Systems Consultant-Cont site				
5012	Sr. Client/Server Developer-onsite	$		$	
5012a	Sr. Client/Server Developer-Cont site				
5013	Business Systems Analyst-onsite	$		$	
5013a	Business Systems Analyst-Cont site				
5014	Training Specialist-onsite	$		$	
5014a	Training Specialist-Cont site				
5015	Sr. Systems Programmer-onsite	$		$	
5015a	Sr. Systems Programmer-Cont site				
5016	Systems Programmer-onsite	$		$	
5016a	Systems Programmer-Cont site				
5017	Analyst/Programmer-onsite	$		$	
5017a	Analyst/Programmer-Cont site				
5018	Documentation Specialist-onsite	$		$	
5018a	Documentation Specialist-Cont site				
5019	Research Analyst-onsite	$		$	
5019a	Research Analyst-Cont site				
5020	Project Administration Staff-onsite	$		$	
5020a	Project Administration Staff-Cont site				
5021	I&A Oper Support Tech III-onsite	$		$	
5021a	I&A Oper Support Tech III-Cont site				
5022	I&A Oper Support Tech II-onsite	$		$	
5022a	I&A Oper Support Tech II-Cont site				
5023	I&A Oper Support Tech I-onsite	$		$	
5023a	I&A Oper Support Tech I-Cont site				
5024	Application Developer III-onsite	$		$	
5024a	Application Developer III-Cont site				
5025	Application Developer II-onsite	$		$	
5025a	Application Developer II-Cont site				
5026	Application Developer I-onsite	$		$	
5026a	Application Developer I-Cont site				
5027	Application Analyst III-onsite	$		$	
5027a	Application Analyst III-Cont site				
5028	Application Analyst II-onsite	$		$	
5028a	Application Analyst II-Cont site				
5029	Application Analyst I-onsite	$		$	
5029a	Application Analyst I-Cont site				

5030	Database Administrator-onsite	$	[redacted]	$
5030a	Database Administrator-Cont site			
5031	Application Operator II-onsite	$		$
5031a	Application Operator II-Cont site			
5032	Application Operator I-onsite	$		$
5032a	Application Operator I-Cont site			
5033	Help Desk Manager-onsite	$		$
5033a	Help Desk Manager-Cont site			
5034	Help Desk III-onsite	$		$
5034a	Help Desk III-Cont site			
5035	Help Desk II-onsite	$		$
5035a	Help Desk II-onsite			
5036	Help Desk I -onsite	$		$
5036a	Help Desk I -Cont site			
5041	Systems Operator-Onsite	$		
5041a	Systems Operator-Cont site			
5042	Security Specialist-Onsite	$		
5042a	Security Specialist-Cont site			
5043	Systems Administrator-Onsite	$		
5043a	Systems Administrator-Cont. site			
5044	Storage Engineer-Onsite	$		
5044a	Storage Engineer-Cont site			
5045	Network Engineer-Onsite	$		
5045a	Network Engineer-Cont site			
5046	Infrastructure Architect-Onsite	$		
5046a	Infrastructure Architect-Cont site			
	Subtotal Labor Cost		[redacted]	$
5037	Open Market ODCs			$
5038	[redacted] G&A on open market ODCs			$
5039	GSA ODCs			$
5040	[redacted] Sub Handling Fee on CTA ODCs			$
	Total ODCs*			$
Total (Labor and ODCs)				$ 6,713,611.80

Task Order total $ 36,227,056.13